JOURNAL OF COMBINATORIAL THEORY, Series A 33, 167–185 (1982)

On the Density of Sequences of Integers the Sum of No Two of which Is a Square. I. Arithmetic Progressions

J. C. LAGARIAS, A. M. ODLYZKO, AND J. B. SHEARER*

Bell Laboratories, Murray Hill, New Jersey 07974

Communicated by R. L. Graham

Received May 13, 1981

The maximal density attainable by a sequence S of positive integers having the property that the sum of any two elements of S is never a square is studied. J. P. Massias exhibited such a sequence with density $\frac{11}{32}$; it consists of 11 residue classes (mod 32) such that the sum of any two such residue classes is not congruent to a square (mod 32). It is shown that for any positive integer n, one cannot find more than $\frac{11}{32}n$ residue classes (mod n) such that the sum of any two is never congruent to a square (mod n). Thus Massias' example has maximal density among those sequences S made up of a finite set of (infinite) arithmetic progressions. A companion paper will bound the maximal density of an arbitrary such sequence S.

1. INTRODUCTION

P. Erdös and D. Silverman (see [3]) posed the problem of determining the maximal density attainable by a set $S = \{s_i\}$ of positive integers having the following property:

NS. *$s_i + s_j$ is not a perfect square whenever $i \neq j$.*

The set S_0 consisting of all $x \equiv 1 \pmod 3$ clearly has property (NS) since there are no squares $\equiv 2 \pmod 3$. Erdös conjectured this set gave the maximal density attainable. J. P. Massias [8] discovered, however, that the set S_1 consisting of all $x \equiv 1 \pmod 4$ together with all $x \equiv 14, 26, 30 \pmod{32}$ has property (NS) and density $\frac{11}{32}$. In the other direction, it is immediate that the density cannot exceed $\frac{1}{2}$, for any square n^2 excludes $\frac{1}{2}$ the positive integers smaller than n^2 because at most one element of each pair $(k, n^2 - k)$ can be in a set S having property (NS), and for each $\varepsilon > 0$ there is a square between x and $(1 + \varepsilon)x$ for large enough x.

The problem of bounding the density of those sequences S which are finite unions of arithmetic progressions and which have property (NS) is

* Current address: University of California, Berkeley, California 94720.

0097-3165/82/050167–19$02.00/0

582a/33/2-4

considered in this paper. In this case S is simply a union of congruence classes for a suitable modulus n. We shall show in Section 2 that such a set has property (NS) if and only if no two congruence classes (not necessarily distinct) sum to a congruence class (mod n) containing a square.

Let $\alpha(n)$ denote the maximal number of congruence classes (mod n) such that no sum of two of them contains a square. We can restate this in graph-theoretic language as follows: Let Q_n be the undirected graph whose vertices are residue classes r (mod n) and for which $\{r_1, r_2\}$ is an edge if and only if $r_1 + r_2$ is a quadratic residue (mod n). Then $\alpha(n)$ is the independence number of this graph. The maximal density attainable for a sequence consisting of congruence classes (mod n) is just $\alpha(n)/n$. Our main result is the following:

THEOREM A. *$\alpha(n) \leqslant \frac{11}{32}n$ with equality if and only if $32|n$. In all other cases $\alpha(n) \leqslant \frac{1}{3}n$.*

This theorem shows that the example of Massias has the largest density attainable among all sets S with property (NS) consisting of a finite number of arithmetic progressions. The proof of Theorem A uses combinatorial arguments to bound the independence number of graphs having certain properties, and number-theoretic arguments to show the graphs Q_n have these properties.

In a companion paper [5], we consider the general problem of bounding from above the density of an arbitrary sequence having property (NS). Let S denote a finite set with all elements $\leqslant n$ which has property (NS), and let

$$d(n) = \max_S(|S|/n)$$

denote the maximum density of such a set in $[1, n]$. In [5] we prove the following result.

THEOREM B. *There exists an absolute constant n_0 such that if $n \geqslant n_0$. then*

$$d(n) \leqslant 0.475.$$

This result is proved using the Hardy–Littlewood circle method, based on an idea suggested by the method used in this paper. Theorem B immediately implies an upper bound of 0.475 for the upper asymptotic density of any infinite sequence S having property (NS).

It is interesting to note that the density behavior of sets S having property (NS) differs radically from those sets S having the following property:

(DS). *$s_i - s_j$ is not a perfect square whenever $i \neq j$.*

Sárközy [10] has shown that any set S having property (DS) must have

density 0, and in fact that the number of elements $\leqslant x$ in such a set is $0\ [x(\log\log x)^{2/3}/(\log x)^{1/3}]$.

The proof of Theorem A is given in Sections 2 and 3, assuming the truth of a number-theoretic result proved in Section 4. In Section 5 we shall outline a proof of the fact that $\alpha(n)\to\infty$ as $n\to\infty$, which answers a question raised by J.-L. Nicolas and provides an interesting complement to Theorem A.

2. Independence Number of Graphs

We first prove that if S is a union of congruence classes modulo n, then S has property (NS) if and only if no two of these congruence classes (not necesarily distinct) sum to a congruence class modulo n that contains a square. The "if" part of this claim is clear. To prove the "only if" part, suppose that S consists of congruence classes (mod n) and for some $s, t\in S$ (not necessarily distinct)

$$s+t\equiv u^2 \pmod n$$

for some $u\in Z^+$. This says that

$$s+t=u^2+kn$$

for some integer k. But then

$$(u+vn)^2=s+t+(2uv+v^2n-k)n,$$

and if v is large enough, we can clearly write

$$(u+vn)^2=(s+in)+(t+jn)$$

for $i,j\in Z^+$, $s+in\neq t+jn$. Since $s+in$ and $t+jn$ are both in S, this shows that S does not satisfy property (NS), which completes the proof of the claim.

Let Q_n denote the graph whose vertices correspond to residues i (mod n) and $\{i,j\}$ is an edge of Q_n if and only if

$$z^2\equiv i+j \pmod n \tag{2.1}$$

has at least one solution z. Q_n is an undirected graph which may contain loops (Fig. 1), but has no multiple edges or multiple loops.

We consider general undirected graphs G which may contain loops, but with no multiple loops at a single vertex or multiple edges. Let $V(G)$, $E(G)$ denote the vertex and edge set of such a graph G, respectively. Let $\alpha(G)$

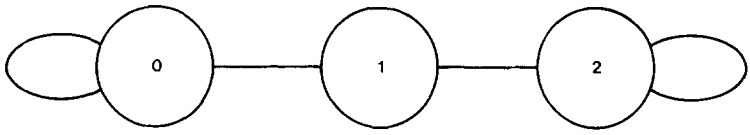

FIG. 1. Q_3.

denote the *independence number* of G, i.e., the maximal number of points having no loops or edges between them. The *independence ratio* $i(G)$ is

$$i(G) = \alpha(G)/|V(G)|,$$

where $|V(G)|$ denotes the number of vertices of G. The *product graph* $G_1 \times \cdots \times G_m$ of m graphs has vertex set $V(G_1 \times \cdots \times G_m) = V(G_1) \times \cdots \times V(G_m)$ and the vertex $(v_1, ..., v_m)$ is adjacent to the vertex $(w_1, ..., w_m)$ iff $\{v_i, w_i\}$ is an edge of G_i for all i.

Product graphs are relevant to the problem at hand for the following reason.

LEMMA 2.1. *Let $n = p_1^{a_1} \cdots p_j^{a_j}$ be the prime factorization of n. Then*

$$Q_n \cong Q_{p_1^{a_1}} \times \cdots \times Q_{p_j^{a_j}}.$$

Proof. Given the vertex $z \pmod n$ of G_n, associate to it the vertex $(z_1, ..., z_j)$ with $z \equiv z_k \pmod{p_k^{a_k}}$ of $Q_{p_1^{a_1}} \times \cdots \times Q_{p_j^{a_j}}$. The Chinese remainder theorem guarantees this is a bijective mapping and that the edge conditions are satisfied, since (2.1) is satisfied if and only if

$$z_k^2 \equiv i + j \pmod{p_k^{a_k}}$$

for all k. ∎

The proof of Theorem A involves obtaining upper bounds for the independence numbers $\alpha(Q_n)$ of the graphs Q_n. This can be done using the following devices. The independence number $\alpha(G)$ of a graph G is the optimal value of the 0-1 integer program $L(G)$ which maximizes the objective function

$$z = \sum_{i \in V(G)} x_i \tag{2.2}$$

subject to

$$x_i + x_j \leqslant 1 \quad \text{if} \quad \{i, j\} \in E(G), \tag{2.3}$$

$$x_i = 0 \quad \text{or} \quad 1 \quad \text{for all} \quad i. \tag{2.4}$$

We can obtain an upper bound for $\alpha(G)$ by solving instead a 0-1 integer programming problem obtained by replacing some of the constraints (2.3) by possibly weaker auxiliary constraints which are valid for all feasible solutions to the system (2.3)–(2.4). An example of an auxiliary constraint is

$$\sum_{i \in V(H)} x_i \leqslant \alpha(H), \tag{2.5}$$

where H is a subgraph of G. We call this device *loosening* the problem. We can also obtain an upper bound for $\alpha(G)$ by subdividing the problem into a collection of subproblems $L_1, \ldots, L_k$ each using only a subset of the constraints and each having an objective function z_j such that

$$\sum_{j=1}^{k} z_j = z.$$

Then adding up the optimal bounds for the subproblems L_i gives an upper bound for the optimal solution of the original problem. We call this device *decomposition* of the problem. Finally, we may obtain upper bounds for $\alpha(G)$ by dropping the 0-1 integer requirements and treating the problem as a linear program. This is *linearization.* We use all of these devices in the proof of Theorem A.

The problem of obtaining upper bounds for the independence number of a graph also arises in connection with the information-theoretic problem of determining the Shannon capacity of a graph G, (c.f., Lovasz [7], Rosenfeld [9], Shannon [11]). The Shannon capacity problem involves the study of the independence number of iterated strong products $G \cdot G \cdot \cdots \cdot G$ of a graph G. (See [7] for a definition of strong product $G \cdot G$. We remark that Rosenfeld [9] studies iterated product graphs $G \times \cdots \times G$ but uses a different definition of independence number of G than that used here. He calls a set of vertices independent if there are no edges between vertices, but loops are allowed.) Rosenfeld [9] obtained bounds using linear programming arguments, while the method of Lovasz [7] implicitly uses some part of the 0-1 integer programming character of the problem. The problem we consider here does not seem susceptible to purely linear programming arguments, and our proofs (particularly Theorem 3.1) make use of the 0-1 constraints.

To begin the proofs, we first add to the list of auxiliary constraints we shall use. When a graph H contains loops, we can obtain stronger constraints than (2.5). When $H = \{1, 1\}$ is a loop, we will utilize the constraint

$$3x_1 \leqslant 1. \tag{2.6}$$

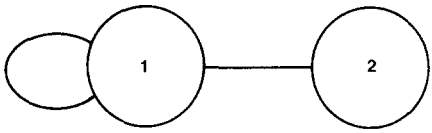

FIG. 2. Collapsed triangle.

When H is a *collapsed triangle* (see Fig. 2) obtained by identifying two vertices of a triangle, we use the constraint

$$2x_1 + x_2 \leqslant 1. \tag{2.7}$$

Actually, the 0-1 conditions force $x_1 = 0$ in these cases, and we use the constraints (2.6), (2.7) because they are compatible with the product operation (see Lemma 2.5). We define the coefficients of the vertex variables appearing in (2.5)–(2.7) to be the *multiplicities* of those vertices in the subgraph H.

We now consider an upper bound for $\alpha(G)$ obtained using loosening and linearization. We say a graph G has a *d-uniform covering by subgraphs* H_j, for $1 \leqslant j \leqslant k$, if each vertex of G occurs exactly d times in the subgraphs H_i, when counted with multiplicity as defined above.

LEMMA 2.2. *If G has a d-uniform covering by subgraphs H_i, $1 \leqslant i \leqslant k$, then*

$$\alpha(G) \leqslant \frac{1}{d} \sum_{i=1}^{k} \alpha(H_i). \tag{2.8}$$

Proof. The coverings give auxilliary constraints of the form (2.5)–(2.7). Adding all these up over all H_i, we obtain the inequality

$$dz = d \sum_{j \in V(G)} x_j \leqslant \sum_{i=1}^{k} \alpha(H_i), \tag{2.9}$$

which implies (2.8). ∎

The lemma has immediate applicability since we have the following result, whose proof is primarily number-theoretic and is deferred to Section 4:

THEOREM 2.3. *Let n be odd. Then Q_n has a d-uniform covering consisting entirely of triangles, collapsed triangles and loops, for some d depending on n.*

COROLLARY 2.4. *Let n be odd. Then $i(Q_n) \leqslant \frac{1}{3}$.*

Proof. By Lemma 2.2

$$\alpha(Q_n) \leqslant \frac{1}{d} \sum_{i=1}^{k} \alpha(H_i) = \frac{k}{d}, \tag{2.10}$$

where H_i is the d-uniform-covering given by Theorem 2.3, since $\alpha(H_i) = 1$ for triangles, collapsed triangles and loops. By counting weighted vertices, the d-uniformity condition implies $k = (d/3)\ |V(Q_n)|$, since each H_i has weight 3. Applying this in (2.10) finishes the proof. ∎

To handle the remaining case of even n, we need to consider the relation of independence ratios of graphs to the product operation. We have the obvious bound

$$i(G) \leqslant i(G \times H) \tag{2.11}$$

for any G, H, by noting $I \times V(H)$ is an independent set of $G \times H$ if I is an independent subset of $V(G)$. Unfortunately, this inequality goes the wrong way for our purposes. We obtain an inequality going the other way for certain d-uniform coverings.

LEMMA 2.5. *Let H have a d-uniform covering H_i, $1 \leqslant i \leqslant k$. consisting entirely of triangles, collapsed triangles, and loops. Then for any graph G*

$$i(G \times H) \leqslant i(G \times T), \tag{2.12}$$

where T is a triangle.

Proof. We prove this by decomposition. Associate to each subgraph $G \times H_i$ the 0-1 integer programming problem L_i which is to maximize the objective function

$$z_i = \sum_{V(G \times H_i)} a_j x_j, \tag{2.13}$$

where if $j = (g, k)$ is a vertex of $G \times H_i$, then a_j is the weight of k viewed as a vertex of H_i. The constraints are that

$$x_j + x_k \leqslant 1 \qquad \text{for all} \quad \{j, k\} \in E(G \times H_i). \tag{2.14}$$

Let $\beta(G \times H_i)$ denote the optimal value of this integer program. The d-uniformity property yields

$$dz = d \sum_{i \in V(G)} x_i = \sum_{i=1}^{k} z_i. \tag{2.15}$$

Thus, the integer programs L_i decompose $L(G)$ so that (2.15) gives

$$\alpha(G) \leqslant \frac{1}{d} \sum_{i=1}^{k} \beta(G \times H_i). \tag{2.16}$$

Now if H_i is a triangle T, then

$$\beta(G \times H_i) = \alpha(G \times T),$$

since all the $\alpha_j = 1$ in (2.13), and (2.13), (2.14) is just the integer programming problem for calculating the independence number.

Next we claim that for a collapsed triangle C,

$$\beta(G \times C) \leqslant \alpha(G \times T). \tag{2.17}$$

This follows since the integer programming problem (2.13), (2.14) L_i for $G \times C$ can be obtained from that for $G \times T$ by adding the additional constraints

$$x_{j_1} = x_{j_2} \tag{2.18}$$

for all $j_1 = (g, 1), j_2 = (g, 3)$, and $g \in V(G)$. Similarly, we obtain that if H_i is a loop L, then

$$\beta(G \times L) \leqslant \alpha(G \times L),$$

since the integer programming problem for $G \times L$ can be obtained from that for $G \times T$ by adding extra constraints.

Thus, (2.16) gives

$$\alpha(G) \leqslant \frac{k}{d} \alpha(G \times T). \tag{2.19}$$

A counting argument gives $k = (d/3)\,|V(G)|$ as in Corollary 2.4, and putting this in (2.19) completes the proof. ∎

By Lemma 2.1, if $n = 2^j m$ and m is odd, $Q_n \cong Q_{2^j} \times Q_m$. Theorem 2.3 and Lemma 2.5, then, show that

$$i(Q_n) \leqslant i(Q_{2^j} \times T), \tag{2.20}$$

where T is a triangle. The set of equivalence classes produced by Massias show that $i(Q_n) \geqslant \frac{11}{32}$ if $32 | n$. Then (2.20) shows that Theorem A will follow if we prove that

$$i(Q_{2^j} \times T) \leqslant \tfrac{11}{32} \tag{2.21}$$

for all j, and that

$$i(Q_{16} \times T) \leqslant \tfrac{1}{3}, \tag{2.22}$$

where T is a triangle.

We next note (2.22) is a consequence of (2.21). Indeed, $Q_{16} \times T$ has 48 vertices, so that $i(Q_{16} \times T)$ is of the form $k/48$ for some integer k. But (2.21) gives $k \leqslant 48\ (\frac{11}{32}) = 16.5$ so $k \leqslant 16$, which is (2.22).

The remaining inequality (2.21) is proved in the next section.

3. An Integer Programming Bound

We have reduced the proof of Theorem A (excluding Theorem 2.3) to the following result:

THEOREM 3.1. *Let T be a triangle. Then*

$$i(Q_{2^n} \times T) \leqslant \tfrac{11}{32}. \tag{3.1}$$

Proof. We will prove the theorem by induction on n. It is easily verified for $n = 1, 2$ so we may take $n \geqslant 3$.

Let $G = Q_{2^n} \times T$ and let I be an independent set in G. Partition the set of vertices of G into 8 classes $V_0, V_1, \ldots, V_7$ indexed by the partition of the vertices of Q_{2^n} into congruence classes (mod 8). Let α_i be the proportion of the elements of V_i that are included in I. The theorem asserts that

$$S = \sum_{i=0}^{7} \alpha_i \leqslant 8 \times \tfrac{11}{32} = 2\tfrac{3}{4}. \tag{3.2}$$

The first half of the proof consists of deducing constraints on the α_i implied by the 0-1 integer constraints. It consists of the following claims (1)–(6).

(1a) $\alpha_0 = 0$ or $\alpha_1 = 0$ or both $\alpha_0 \leqslant \frac{1}{3}$ and $\alpha_1 \leqslant \frac{1}{3}$,

(1b) $\alpha_2 = 0$ or $\alpha_7 = 0$ or both $\alpha_2 \leqslant \frac{1}{3}$ and $\alpha_7 \leqslant \frac{1}{3}$,

(1c) $\alpha_3 = 0$ or $\alpha_6 = 0$ or both $\alpha_3 \leqslant \frac{1}{3}$ and $\alpha_6 \leqslant \frac{1}{3}$,

(1d) $\alpha_4 = 0$ or $\alpha_5 = 0$ or both $\alpha_4 \leqslant \frac{1}{3}$ and $\alpha_5 \leqslant \frac{1}{3}$,

(2) $\alpha_0 + \alpha_4 \leqslant \frac{11}{16}$,

(3a) $\alpha_1 + \alpha_3 \leqslant 1$,

(3b) $\alpha_5 + \alpha_7 \leqslant 1$,

(4a) $\alpha_1 + \alpha_7 \leqslant 1$,

(4b) $\alpha_3 + \alpha_5 \leqslant 1$,

(5) $2\alpha_2 + \alpha_6 \leqslant 1$,

(6) $2\alpha_6 \leqslant 1$.

Besides these, we have the obvious constraints:

(7) $0 \leqslant \alpha_i \leqslant 1$ for $i = 0, 1, \ldots, 7$.

To prove claim (1), let the vertices of the triangle T be denoted a, b, c. Suppose $\alpha_0 \neq 0$, then I contains an element of V_0 which we make take to be (x, a) with $x \equiv 0 \pmod 8$. Then I cannot contain any elements (y, b) or (y, c) with $y \equiv 1 \pmod 8$ since all $y \pmod{2^n}$ with $y \equiv 1 \pmod 8$ are quadratic residues. Hence, $\alpha_1 \leqslant \frac{1}{3}$. Similarly, $\alpha_j \neq 0$ implies $\alpha_{1-j} \leqslant \frac{1}{3}$, where the indices of α are taken modulo 8. This proves claim (1).

Claim (2) follows from the induction hypothesis since the induced subgraph on the vertices $V_0 \cup V_4$ is isomorphic to $Q_{2^{n-2}} \times T$.

To prove claim (3a), we exhibit a matching between V_1 and V_3. Consider the edges $\{(x, a), (4-x, b)\}$, $\{(x, b), (4-x, c)\}$, and $\{(x, c), (4-x, a)\}$ for all $x \pmod{2^n}$ with $x \equiv 1 \pmod 8$. These edges have the property that each vertex of V_1 present in I excludes a matching one of V_3 and vice versa. This proves (3a). If we let $x \equiv 5 \pmod 8$ instead we obtain a matching between V_5 and V_7, which proves (3b).

To prove claim (4a) we exhibit a matching between V_1 and V_7. This is $\{(x, a), (-x, b)\}$, $\{(x, b), (-x, c)\}$, $\{(x, c), (-x, a)\}$ for all $x \equiv 1 \pmod 8$. Taking $x \equiv 5 \pmod 8$ gives a matching of V_3 and V_5 proving claim (4b).

To prove claim (5) we shall consider the induced subgraph on $V_2 \cup V_6$. Consider the triangles $\{(-2x, a), (2x, b), (2x, c)\}$, $\{(-2x, b), (2x, c), (2x, a)\}$, $\{(-2x, c), (2x, a), (2x, b)\}$, $\{(6x, a), (-6x, b), (10x, c)\}$, $\{(6x, b), (-6x, c), (10x, a)\}$, $\{(6x, c), (-6x, a), (10x, b)\}$ as $x \pmod{2^n}$ runs over all residues $\equiv 1 \pmod 8$. These triangles lie in the induced subgraph and each gives a constraint

$$x_{i_1} + x_{i_2} + x_{i_3} \leqslant 1.$$

Adding up these constraints over all these triangles, we note each vertex of V_6 is covered twice and each vertex of V_2 exactly four times, so we obtain

$$2 \sum_{i \in V_6} x_i + 4 \sum_{i \in V_2} x_i \leqslant 6 \times 2^{n-3}. \tag{3.3}$$

Dividing this by $6 \times 2^{n-3}$ gives (5).

To prove claim (6) for $n \geqslant 4$ we give a matching of half the vertices in C_6 to the other half. We pair $\{(x, a), (4-x, b)\}$, $\{(x, b), (4-x, c)\}$ and $\{(x, c),$

$(4-x, a)\}$ over all $x \equiv 6 \pmod{16}$. This pairs the vertices with first entry $\equiv 6 \pmod{16}$ against those $\equiv 14 \pmod{16}$ and proves (6) whenever $n \geqslant 4$. In the case $n = 3$ there are 3 vertices in C_6 and the three edges above form a triangle, yielding $3\alpha_6 \leqslant 1$ which trivially implies (6).

The second half of the proof consists of showing that the constraints (1)–(7) imply that $S = \sum_{i=0}^{7} \alpha_i \leqslant 2\frac{3}{4}$. As a preliminary step, we claim that the inequalities (8)–(11) below follow from (1)–(7).

$$\text{(8a)} \quad \alpha_0 + \alpha_1 \leqslant 1,$$
$$\text{(8b)} \quad \alpha_2 + \alpha_7 \leqslant 1,$$
$$\text{(8c)} \quad \alpha_3 + \alpha_6 \leqslant 1,$$
$$\text{(8d)} \quad \alpha_4 + \alpha_5 \leqslant 1,$$
$$\text{(9)} \quad \alpha_2 + \alpha_6 \leqslant \tfrac{3}{4},$$
$$\text{(10a)} \quad \alpha_2 + \alpha_6 + \alpha_1 + \alpha_3 + \alpha_7 \leqslant 2,$$
$$\text{(10b)} \quad \alpha_2 + \alpha_6 + \alpha_3 + \alpha_5 + \alpha_7 \leqslant 2,$$
$$\text{(11a)} \quad \alpha_0 + \alpha_4 + \alpha_1 + \alpha_3 + \alpha_5 \leqslant 2,$$
$$\text{(11b)} \quad \alpha_0 + \alpha_4 + \alpha_1 + \alpha_5 + \alpha_7 \leqslant 2.$$

Claims (8a)–(8d) are immediate consequences of (1a)–(1d). Claim (9) follows from (5) and (6). To prove claim (10a), we consider several cases. Suppose $\alpha_3 = 0$. Then

$$\alpha_2 + \alpha_6 + \alpha_1 + \alpha_3 + \alpha_7 = (\alpha_2 + \alpha_6) + (\alpha_1 + \alpha_7) \leqslant 1 + \tfrac{3}{4} < 2,$$

using (9) and (4a). Similarly, (10a) is true if $\alpha_7 = 0$ using (9) and (3a). If $\alpha_2 = 0$, then

$$\alpha_2 + \alpha_6 + \alpha_1 + \alpha_3 + \alpha_7 = (\alpha_3 + \alpha_6) + (\alpha_1 + \alpha_7) \leqslant 2,$$

using (8c) and (4a). Similarly, (10a) is true if $\alpha_6 = 0$ using (8b) and (3a). Hence, we may suppose $\alpha_2, {}_3, \alpha_6, \alpha_7$ are all nonzero. Then (1b), (1c) imply $\alpha_2, \alpha_3, \alpha_6, \alpha_7$ are each $\leqslant \frac{1}{3}$. But then $(\alpha_1 + \alpha_7) + \alpha_2 + \alpha_3 + \alpha_6 \leqslant 2$ using this fact and (4a). This proves (10a). Claim (10b) has a similar proof.

To prove claim (11a), we again consider several cases. Suppose $\alpha_5 = 0$. Then

$$\alpha_0 + \alpha_4 + \alpha_1 + \alpha_3 + \alpha_5 = (\alpha_0 + \alpha_4) + (\alpha_1 + \alpha_3) \leqslant \tfrac{11}{16} + 1 < 2.$$

using (2), (3a). Similarly, (11a) is true if $\alpha_1 = 0$ because of (2), (4b). Suppose $\alpha_4 = 0$. Then

$$\alpha_0 + \alpha_4 + \alpha_1 + \alpha_3 + \alpha_5 = (\alpha_0 + \alpha_1) + (\alpha_3 + \alpha_5) \leqslant 2,$$

using (8a) and (4b). Similarly, (11a) is true if $\alpha_0 = 0$ because of (8d) and

(3a). Hence, we may suppose $\alpha_0, \alpha_1, \alpha_4, \alpha_5$ are all nonzero. Then (1a), (1d) imply $\alpha_0, \alpha_1, \alpha_4, \alpha_5$ are all $\leqslant \frac{1}{3}$. But then $(\alpha_1 + \alpha_3) + \alpha_0 + \alpha_4 + \alpha_5 \leqslant 2$ using this fact and (3a). This proves (11a). Claim (11b) has a similar proof.

We can now verify that (3.2) holds. Suppose first that all the α_i are nonzero. Then by (1) all $\alpha_i \leqslant \frac{1}{3}$ so $S \leqslant \frac{8}{3} < \frac{11}{4}$. Suppose next that $\alpha_1 = 0$. Then

$$S = (\alpha_0 + \alpha_4) + (\alpha_2 + \alpha_6 + \alpha_3 + \alpha_5 + \alpha_7) \leqslant \tfrac{11}{16} + 2 < \tfrac{11}{4},$$

using (2) and (10b). Similarly (3.2) holds whenever $\alpha_5 = 0$ using (2) and (10a). If $\alpha_7 = 0$ or $\alpha_3 = 0$, then (3.2) follows from (9) and (11a) or (9) and (11b), respectively. So suppose next $\alpha_1, \alpha_3, \alpha_5, \alpha_7$ are all nonzero. Then using (1) we have $\alpha_0, \alpha_2, \alpha_4, \alpha_6$ are all $\leqslant \frac{1}{3}$. Hence, if two or more of $\alpha_0, \alpha_2, \alpha_4, \alpha_6$ are zero we have

$$S = (\alpha_1 + \alpha_3) + (\alpha_5 + \alpha_7) + (\alpha_0 + \alpha_2 + \alpha_4 + \alpha_6) \leqslant \tfrac{8}{3},$$

using (3a), (3b). The remaining cases to consider are those where exactly one of $\alpha_0, \alpha_2, \alpha_4, \alpha_6$ is zero. Suppose $\alpha_0 = 0$ and the remaining seven $\alpha_i \neq 0$. Then $\alpha_2, \alpha_3, \alpha_4, \alpha_5, \alpha_6, \alpha_7 \leqslant \frac{1}{3}$ using (1). In this case,

$$S = (\alpha_1 + \alpha_7) + \alpha_2 + \alpha_3 + \alpha_4 + \alpha_5 + \alpha_6 \leqslant 1 + \tfrac{5}{3} = \tfrac{8}{3},$$

using (4a). Similar arguments work when exactly one of $\alpha_2, \alpha_4, \alpha_6 = 0$ and all other $\alpha_i \neq 0$, using (4a), (4b), (4b), respectively. This shows (3.2) always holds, and completes the induction step. ∎

4. Some Uniform Coverings

We shall prove Theorem 2.3 via a series of lemmas.

LEMMA 4.1 *Let G_1 have a d_1-uniform covering consisting of triangles, collapsed triangles and loops, and G_2 a d_2-uniform covering of triangles and loops. Then $G_1 \times G_2$ has a $2d_1d_2$-uniform covering of triangles, collapsed triangles, and loops.*

Proof. Let H_i be the graphs involved in the d_1-uniform covering of G_1, K_j that of G_2. We shall cover each $H_i \times K_j$ separately with triangles T, collapsed triangles C, and loops L to achieve $2d_1d_2$-uniformity. $T \times T$ has a 2-uniform covering by 6 triangles, these triangles being $\{(1, \sigma(1)), (2, \sigma(2)), (3, \sigma(3)): \sigma \in S_3\}$. Let T denote a triangle, C a collapsed triangle, and L a loop. For any graph G, $G \times L \cong G$, so we get a 2-uniform covering of $L \times L$, $C \times L$, $T \times L$ by 2 copies of L, G, T, respectively. The remaining case that can occur is $C \times T$. This has a 1-uniform covering by three triangles in which the vertices of $C \times T$ corresponding to the loop in C are each covered

twice, the others once. We associate two copies of this covering to $C \times T$, using six triangles in all. It is straightforward to check that the collection of triangles, collapsed triangles, and loops so obtained is a $2d_1d_2$-uniform covering of $G_1 \times G_2$. (Recall that the multiplicities of vertices in C, L must be taken into account.) ∎

We shall establish that G_{p^n} has a 2-uniform covering with triangles, collapsed triangles, and loops if $p = 3$, and a 6-uniform covering with just triangles and loops for all other primes p. Then Lemma 2.1 and repeated application of Lemma 4.1 complete the proof of Theorem 2.3.

We first treat some special cases.

LEMMA 4.2. *Q_{p^n} has a 2-uniform covering with triangles and collapsed triangles for $p = 3$, and a 3-uniform covering by triangles and loops for $p = 5, 11$.*

Proof. In checking the following constructions, the fact to keep in mind is that if $y \pmod{p^n}$ has $y \pmod{p}$ a nonzero quadratic residue $\pmod{p}$, then y is a quadratic residue $\pmod{p^n}$.

For $p = 3$, use the triangles

$$(2 + 3k, 2 + 3k, -2 - 3k), \tag{4.1a}$$

$$(1 + 3k, 3k, -3k), \tag{4.1b}$$

for $1 \leqslant k \leqslant 3^{n-1}$. ((4.1b) is a collapsed triangle when $k = 3^{n-1}$.) This is a 2-uniform covering of Q_{3^n}.

For $p = 5$, use the triangles

$$(5k, 1 + 5k, -1 - 5k)$$

for $1 \leqslant k \leqslant 5^{n-1}$, repeated 3 times each, and the loops

$$(2 + 5k, 2 + 5k)$$

$$(3 + 5k, 3 + 5k)$$

for $1 \leqslant k \leqslant 5^{n-1}$, each occurring once. This is a 3-uniform covering of Q_{5^n}.

For $p = 11$ let (a, b, c) stand for $(a + 11k,\ b + 11k,\ c + 11k)$ for $1 \leqslant k \leqslant 11^{n-1}$. A 3-uniform covering by triangles and loops is given by $(0, 1, 3)$, $(0, 3, 9)$, $(0, 5, 9)$, $(5, 7, 9)$, $(1, 4, 8)$, $(2, 2, 2)$, $(6, 6, 6)$, $(10, 10, 10)$, and

$$(1 + 11k, 3 + 11k, -3 - 11k), \qquad (5 + 11k, 4 + 11k, -4 - 11k),$$

$$(8 + 11k, 4 + 11k, -4 - 11k)$$

for $1 \leqslant k \leqslant 11^{n-1}$. ∎

For all other primes p we use a general construction. It is based on the following lemma:

LEMMA 4.3. *For $p = 7$ and all primes $p \geqslant 13$, there exist triples (x_1, x_2, x_3) and (y_1, y_2, y_3) (mod p) such that*

(1) *x_i, y_i are both nonzero quadratic residues (mod p) for $1 \leqslant i \leqslant 3$.*

(2) *$x_i + x_j$ is a quadratic residue if $i \neq j$.*

(3) *$y_i + y_j$ is a quadratic nonresidue if $i \neq j$.*

(4) *x_1, x_2, x_3 are either all equal or all distinct.*

(5) *y_1, y_2, y_3 are either all equal or all distinct.*

Proof. (i) For the x_i take $(117^2, 44^2, 240^2)$. Then each sum is a perfect square (Sierpinski [12, p. 61]). The x_i have no prime factors >13 and are distinct modulo primes $\neq 2, 3, 7, 17, 23, 41, 71, 73$. For $p = 7$, take $(x_1, x_2, x_3) = (1, 1, 1)$, for $p = 13$ take $(1, 3, 9)$ and for $p = 17, 23, 41, 71$, and 73, take $(x_1, x_2, x_3) = (1, 1, 1)$.

(ii) For the y_i, let λ be a quadratic nonresidue (mod p), and consider the simultaneous system of congruences

$$w_1^2 + 1 \equiv \lambda z_1^2 \pmod{p}, \tag{4.2}$$

$$w_2^2 + 1 \equiv \lambda z_2^2 \pmod{p}, \tag{4.3}$$

$$w_1^2 + w_2^2 \equiv \lambda z_3^2 \pmod{p}. \tag{4.4}$$

The Lang–Weil bounds [6] guarantee this system has $p^2 + O(p^{3/2})$ solutions, and at most $O(p)$ solutions have w_1, w_2, z_1, z_2 or $z_3 \equiv 0 \pmod{p}$, so that for sufficiently large p we can find a solution with w_1, w_2, z_1, z_2, z_3 all $\not\equiv 0 \pmod{p}$. Then we can take $(y_1, y_2, y_3) = (1, w_1^2, w_2^2)$. If $y_i = y_j$ for some $i \neq j$, then we choose instead (y_i, y_i, y_i).

We need the explicit bound $p \geqslant 13$, and use character sum arguments to obtain it. Let $\chi(n) = (n/p)$ be the Legendre symbol. We first claim that for $p > 2$ there exists a solution pair (w_1, z_1) to $w_1^2 + 1 \equiv \lambda z_1^2$ such that $w_1 z_1 \not\equiv 0$. (All equation and variables are taken modulo p here.) The equation $z^2 \equiv w_1^2 + 1$ has exactly $p - 1$ solution pairs (z, w_1) since we can write

$$(z - w_1)(z + w_1) \equiv 1$$

so for all $a \not\equiv 0 \pmod{p}$ we obtain a solution pair by solving

$$z - w_1 \equiv a, \qquad z + w_1 \equiv 1/a.$$

Now the equations

$$\lambda z_1^2 \equiv w_1^2 + 1, \tag{4.5}$$

$$z_2^2 \equiv w_1^2 + 1, \tag{4.6}$$

have between them exactly $2p$ solutions since for each $w_1 \pmod p$ with $w_1^2 \not\equiv -1 \pmod p$, either (4.5) or (4.6) is solvable, and there are two solutions z_i to that equation. (If $w_1^2 \equiv -1 \pmod p$ both (4.5) and (4.6) are solvable with one solution each.) Thus, (4.5) has $p+1$ solutions, at most 2 of which have $w_1 z_1 \equiv 0 \pmod p$, proving the claim.

Now pick nonzero w_1, z_1 solving (4.2) and fix these in the sequel. Let

$$S = \sum_{w_2=0}^{p} (1 - \chi(w_2^2 + 1))(1 - \chi(w_2^2 + w_1^2)).$$

Each term in the sum S is $\geqslant 0$ and is 4 if w_2^2+1, $w_2^2+w_1^2$ are both quadratic nonresidues, 0 if either w_1^2+1 or w_2^2+1 is a nonzero quadratic residue, and is $\leqslant 2$, otherwise. The exceptional cases arise when $w_2^2 + 1 \equiv 0 \pmod p$ or $w_2^2 + w_1^2 \equiv 0 \pmod p$ which can occur for at most 4 values of w_2. Hence

$$S \leqslant 8 + T, \tag{4.7}$$

where T is the number of solutions of

$$w_2^2 + 1 \equiv \lambda z_2^2, \qquad w_2^2 + w_1^2 \equiv \lambda z_3^2,$$

with z_2, z_3 both $\not\equiv 0 \pmod p$. By direct calculation

$$\begin{aligned} S &= p - \sum_{w_2=0}^{p} \chi(w_2^2+1) - \sum_{w_2=0}^{p} \chi(w_2^2+w_1^2) + \sum_{w_2=0}^{p} \chi((w_2^2+1)(w_2^2+w_1^2)) \\ &\equiv p - C_1 - C_2 + C_3. \end{aligned} \tag{4.8}$$

Since there are $p-1$ solution pairs (x, w_2) to $x^2 \equiv w_2 + 1 \pmod p$, and each w_2 appearing in such a pair appears with two different x's, except when $w_2^2 \equiv -1 \pmod p$, we conclude that if -1 is a quadratic nonresidue, C_1 contains $(p-1)/2$ terms equal to $+1$, and $(p+1)/2$ equal to -1. If -1 is a quadratic residue, C_1 contains 2 terms equal to 0, $(p-3)/2$ equal to $+1$, and $(p-1)/2$ equal to -1. In either case,

$$C_1 = -1$$

and

$$C_2 = \sum_{w_2=0}^{p} \chi(w_2^2 + w_1^2) = \chi(w_1^2) \sum_{u_2=0}^{p} \chi(u_2^2 + 1) = C_1 = -1. \tag{4.9}$$

For C_3, suppose first $w_1^2 \equiv 1$. Then note $(y_1, y_2, y_3) = (1, 1, 1)$ has the required property, so we may exclude this case in what follows. Now

$$w_1^2 + 1 \equiv \lambda z_1^2, \qquad z_1 \not\equiv 0, \tag{4.10}$$

shows $w_1^2 \equiv 0$ cannot occur. If $w_1^2 \equiv -2$, then for (4.10) to be solvable we must have $(-1/p) = -1$. Then

$$(2/p) = (-2/p)(-1/p) = -1,$$

so that $(y_1, y_2, y_3) = (1, 1, 1)$ satisfies the conditions of the lemma, and we may exclude this case.

Now view the curve

$$y^2 = (w_2^2 + 1)(w_2^2 + w_1^2) \tag{4.11}$$

with w_1^2 fixed as an elliptic curve. Using formulae in Adams and Razar [1], its discriminant Δ may be calculated to be (up to powers of 2 and 3)

$$\Delta = 2^4 3^2 (w_1^2)(w_1^2 - 1)^2 (w_1 + 2)^2.$$

Hence, if $w_1^2 \equiv 0, 1, -2 \pmod p$ the curve (4.11) has good reduction (mod p) and is a nonsingular elliptic curve.

Suppose (4.11) has s_1 solutions. Then

$$\lambda y^2 \equiv (w_2^2 + 1)(w_2^2 + w_1^2)$$

has

$$s_2 = 2p - s_1 \tag{4.12}$$

solutions (mod p). The Weil bound is

$$|s_1 - p| < 2\sqrt{p}, \tag{4.13}$$

where p occurs instead of $p + 1$ in this formula since (4.11) has exactly one point at infinity over Z/pZ. Hence

$$|C_3| \leqslant \tfrac{1}{2}|s_1 - s_2| + 1 \leqslant 2\sqrt{p} + 1, \tag{4.14}$$

using (4.12), (4.13).

Combining (4.8) with these bounds for the C_i, we have

$$S \geqslant p + 2 - |C_3| \geqslant p - 2\sqrt{p} + 1.$$

Then (4.7) gives

$$T \geqslant p - 2\sqrt{p} - 7,$$

which shows $T > 0$ for $p \geqslant 17$. For $p = 7$ we take $(y_1, y_2, y_3) = (1, 2, 4)$, for $p = 13$ we take $(1, 1, 1)$. ∎

We now give the final construction.

LEMMA 4.4. *Let $p = 7$ or any prime $\geqslant 13$. Then Q_{p^n} has a 6-uniform covering by triangles and loops.*

Proof. Take the triple (x_1, x_2, x_3) that exists for such p by Lemma 4.3. Since all $x_i \not\equiv 0 \pmod p$, each $x_i + a_i p$ is a quadratic residue $(\bmod p^n)$ for any choice of a_i. At most two of the pairs (i, j) with $i < j$ can have $x_i + x_j \equiv 0 \pmod p$, so we can choose a_i to guarantee that for these pairs $x_i + x_j + a_i p + a_j p \equiv 0 \pmod{p^n}$, i.e., without loss of generality we may suppose all $x_i + x_j$ with $i \neq j$ are quadratic residues $(\bmod p^n)$. Let μ be a fixed integer which is a quadratic nonresidue $(\bmod p)$.

The 6-uniform covering $(\bmod p^n)$ is given by taking the triple $(0, 0, 0)$ twice (this is a loop), the sets

$$(ap, -ap, x_1 + ap), \qquad (ap, -ap, x_2 + ap), \qquad (ap, -ap, x_3 + ap)$$

for $1 \leqslant a \leqslant p^{n-1} - 1$, the sets

$$\lambda(x_1, x_2, x_3),$$

where λ runs through all $p^{n-1}((p-1)/2)$ invertible quadratic residues twice, except the set of such $\lambda \equiv 1 \pmod p$ are run through exactly once. Finally we use

$$\lambda(\mu y_1, \mu y_2, \mu y_3),$$

where λ runs through all invertible quadratic residues $(\bmod p^n)$ twice, and (y_1, y_2, y_3) comes from Lemma 4.3. Note that μy_1, μy_2, μy_3 are nonzero quadratic nonresidues $(\bmod p)$ whose pairwise sums are invertible quadratic residues $(\bmod p)$, hence, quadratic residues $(\bmod p^n)$.

Lemma 4.3 guarantees that these triples give either triangles or loops in Q_{p^n}, and counting arguments show all vertices are covered exactly six times each. ∎

5. A Lower Bound for the Independence Number

So far this paper has obtained upper bounds for the independence number $\alpha(n)$ of the graph Q_n. In general, determining $\alpha(n)$ for a given n seems to be a very difficult problem. We can prove, however, that $\alpha(n) \to \infty$ as $n \to \infty$. In fact, the proof we sketch here shows that $\alpha(n) \geqslant c \log n$ for some fixed

$c > 0$. On the other hand, reasoning by analogy with related number theoretic problems, it seems reasonable to conjecture that when p is a prime, $\alpha(p) = O((\log p)^2)$, and perhaps even $\alpha(p) = O((\log p)^{1+\varepsilon})$ for every $\varepsilon > 0$.

To show that $\alpha(n) \to \infty$ as $n \to \infty$, we use the fact (equivalent to (2.11)) that for any positive integers k and m,

$$\alpha(km) \geqslant k\alpha(m). \tag{5.1}$$

Therefore, since the largest prime power dividing n tends to infinity as $n \to \infty$, it suffices to prove that $\alpha(p^a) \to \infty$ as $p^a \to \infty$, with p a prime, $a \in Z^+$. But by (5.1), for $a \geqslant 2$,

$$\alpha(p^a) \geqslant p^{a-1}\alpha(p),$$

so it suffices to show that $\alpha(p) \to \infty$ as $p \to \infty$. To prove this last fact, suppose that $S = \{s_1, \ldots, s_k\}$ is an independent set in Q_p; i.e., for $1 \leqslant i, j \leqslant k$,

$$s_i + s_j \not\equiv z^2 \pmod{p}$$

for any z. We will show that if k is small, we can find another integer x such that $S \cup \{x\}$ is an independent set. To do this, we use a variant of the method of [4]. Form

$$g(S) = \sum_{\substack{x=0 \\ x, -x \notin S}}^{p-1} \prod_{j=1}^{k} [1 - \chi(x + s_j)]. \tag{5.2}$$

Each of the summands is 0 if $x + s_j \equiv z^2 \pmod{p}$ for some j, z and is 2^k, otherwise. Hence $g(S) > 0$ if and only if there is an $x \notin S$ such that $S \cup \{x\}$ is an independent set. But now we expand the products in (5.2), collect terms, and apply the Burgess [2] character sum estimates. As in [4], we find that

$$g(S) \geqslant p - 2[(k-2)\,2^{k-1} + 1]\sqrt{p} - k2^{k+1}.$$

If $p > k^2 2^{2k+2}$, $g(S) > 0$, and so S cannot be a maximal independent set. Therefore, $\alpha(p) \geqslant c \log p$ for some fixed $c > 0$.

REFERENCES

1. W. W. ADAMS AND M. RAZAR, Multiples of points on elliptic curves and continued fractions, *Proc. London Math. Soc.* **41** (1980), 481–498.
2. D. A. BURGESS, On character sums and primitive roots, *Proc. London Math. Soc.* (3) **12** (1962), 179–192.
3. P. ERDÖS AND R. L. GRAHAM, Old and new problems and results in combinatorial number theory, *Monogr. l'Enseignement Mathe.* **28** (1980).

4. R. L. GRAHAM AND J. H. SPENCER, A constructive solution to a tournament problem, *Canad. Math. Bull.* **14** (1971), 45–48.
5. J. C. LAGARIAS, A. M. ODLYZKO, AND J. B. SHEARER, On the density of sequences of integers the sum of no two of which is a square II. General sequences, *J. Combin. Theory* Ser. A, to appear.
6. S. LANG AND A. WEIL, Number of points of varieties in finite fields, *Amer. J. Math.* **76** (1954), 819–827.
7. L. LOVASZ, On the Shannon capacity of a graph, *IEEE Trans. Inform. Theory* **IT-25** (1979), 1–8.
8. J. P. MASSIAS, Sur les suites dont les sommes des termes 2 a 2 ne sont pas des carres, to be published.
9. M. ROSENFELD, On a problem of Shannon, *Proc. Amer. Math. Soc.* **18** (1967), 315–319.
10. A. SÁRKÖZY, On difference sets of sequences of integers, I, *Acta Math. Acad. Sci. Hungar.* **31** (1978), 125–149, **MR 57** 5942.
11. C. E. SHANNON, The zero-error capacity of a noisy channel, *IRE Trans. Inform. Theory* **IT-2** (1956), 8–19.
12. W. SIERPÍNSKI, Elementary Theory of Numbers, Warsaw: Polish Scientific Publishers, 1964.